REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
16-04-2013	Master of Military Studies Research Paper	September 2009 - April 2010

4. TITLE AND SUBTITLE
Operational Art in Cyber Defense

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Alanis, Oscar, Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
Upon the establishment of a JTF, a Commander assumes significant risk in the cyber domain. Limited understanding of the characteristics within the cyber domain and lack of clearly defined command and control relationships places the Joint Task Force at excessive risk. Additionally, the Department of Defense relies on the civilian Internet for many supporting functions. Connections to the Internet provide adversaries a direct avenue of approach to target and disrupt Joint Operations. A Commander must benefit from proper command and control structures and improved understanding of the cyber defense situation during Phase 0 to lay the proper foundation prior to conducting an operation. The Department of Defense remains vulnerable unless it can change how the military services are organized, trained and equipped to provide a JTF Commander the means to defend the his networks better.

15. SUBJECT TERMS
Cyber Defense; Operational Art; Cyber Component; JFCCC; JTF Commander; Warfighting Principles; Cyber Space; MOOSEMUS; Computer; Risk; Social Media

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU		Marine Corps University / Command and Staff College
Unclass	Unclass	Unclass			19b. TELEPONE NUMBER (*Include area code*) (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
Operational Art in Cyber Defense

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:

Major Oscar Alanis, USMC

AY 12-13

Mentor and Oral Defense Committee Member: Dr. Richard L. DiNardo
Approved: Richard L. DiNardo
Date: 11 April 2013

Oral Defense Committee Member: Francis H. Marlo
Approved: Francis H. Marlo
Date: 11 April 2013

Executive Summary

Title: Operational Art in Cyber Defense

Author: Major Oscar Alanis, United States Marine Corps

Thesis: Since cyberspace is a warfighting domain, a Joint Task Force (JTF) Commander can use traditional warfighting principles to develop a cyber defense plan as part of an integrated joint campaign once he has clearly established command and control structures.

Discussion: Upon the establishment of a JTF, a Commander assumes significant risk in the cyber domain. Limited understanding of the characteristics within the cyber domain and lack of clearly defined command and control relationships places the Joint Task Force at excessive risk. Additionally, the Department of Defense relies on the civilian Internet for many supporting functions. Connections to the Internet provide adversaries a direct avenue of approach to target and disrupt Joint Operations. A Commander must benefit from proper command and control structures and improved understanding of the cyber defense situation during Phase 0 to lay the proper foundation prior to conducting an operation. The Department of Defense remains vulnerable unless it can change how the military services are organized, trained and equipped to provide a JTF Commander the means to defend the his networks better.

Conclusion: A Joint Task Force Commander can use operational art to defend the cyber domain in support of an integrated campaign plan as he would in any of the other warfighting domains. However, there needs to be a greater understanding within the operations community of the domain's characteristics to improve the combat effectiveness of a JTF. The Department of Defense will need change how the military services organize, train and equip to support a theater campaign by providing a Joint Task Force Commander the tools he needs to prevent the cyber domain from becoming a critical vulnerability.

DISCLAIMER

Table of Contents

Preface

I had the privilege of serving as a Plans and Liaison Officer and the Chief of Computer Network Defense for the Defense Information Systems Agency (DISA) in Germany (DISA-Europe). While there, I learned a great deal about defending the Cyber Domain. It was clear that many questions remained unanswered regarding command and control relationships and providing a Joint Force Commander the support and information he needs to achieve his objectives. As the opportunity presented itself at Marine Corps University, I could dedicate time to read and think about what others had written about cyberwar, cyber warfare, war in cyber and simply war. All of the terms have different meanings to the authors and readers alike. The more I researched the project, the clearer it became to me that warfare in the cyber domain is only a part of war.

As a Certified Information Systems Security Professional, a Certified Information Security Manager and most importantly a US Marine, I felt compelled to try to make sense of how an operational planner and a cyber defense planner could come to common ground in providing an ideal plan to support a common Commander. Both camps have come a long way to understand each other. But much more needs to be done. While there is a great deal of interest in the subject, a definitive solution to how the Department of Defense develops its cyber defense concepts and underpinning doctrine lack substance to adequately protect the networks that support operations. While there is nothing mystical about the domain, there is a danger in having only a cursory understanding of what is possible which may make matters worse before they get better.

I want to express my gratitude to Dr. Richard DiNardo for taking the time to guide me during this work. His perspective in trying to develop what Operational Art in the Cyber domain

might look like in the future was invaluable. I would also like to thank Dr. Frank Marlo, Dr. Matthew Flynn, Paul K. Van Riper, LtGen, USMC (Ret.), LtCol Mike Phillips, USMC and LtCol Paul Melchior, USMC for exposing me to different perspectives when researching the subject. The staff of the Gray Research Center in Quantico is truly a world-class resource that I was extremely fortunate to benefit from. Most importantly, I would like to thank my wife and children for allowing me the time to work through this project and satisfy a personal curiosity.

I used the masculine when referring to the Commander and the adversary throughout this paper for brevity.

Looking for a Functional Cyber Component Command?

A Geographic Combatant Commander has many options when considering how to organize for an operation within his area of responsibility. He can establish a Joint Task Force (JTF) with functional component commands including a land component command, an air component command, and a maritime component command to meet the requirements of an operation. Like the other domains, the cyber domain presents a Commander with both opportunities and pitfalls. Upon the establishment of a JTF, the Commander assumes significant risk in the cyber domain. Networks are designed to share information and are inherently unsecure. The JTF Commander may want to prepare his cyber defense posture to address the threats awaiting him as the operation unfolds. Limited understanding of the characteristics of the domain and a lack of clearly defined command and control relationships within the domain places the JTF at excessive risk. Since cyberspace is a warfighting domain, a JTF Commander can use traditional warfighting principles to develop a cyber defense plan as part of an integrated joint campaign once he has clearly established command and control structures.

What would be the best way to organize a JTF to meet the challenges of the cyber domain? Normally, a functional component command is the service component command with the preponderance of forces in the theater. But, where should a Commander look to establish a Functional Cyber Component Command? Determining how to assign a Functional Cyber Component Command is not as trivial as it sounds. How would a JTF Commander conclude which service component has the preponderance of cyber forces? A JTF Commander cannot simply count how many firewalls and computer security devices each of the service components brings to the fight to determine which component should assume the responsibility. A JTF Commander should not bear the burden of trying to figure this out on his own. The Department

of Defense should establish a framework where a JTF Commander can quickly benefit from a Functional Cyber Component Command prior to a crisis occurring.

Unfortunately, cyber defense organizations within the service components are not organized as traditional military formations. All of the military departments and supporting agencies have varying cyber formations and capabilities with equally unique command and control relationships for their respective commands. Each of the service cyber organizations within a JTF is under the technical control and often the operational control of its respective service headquarters or service cyber component headquarters.

In the case of the Marine Corps, the cyber defense organizations embedded within a Marine Air Ground Task Force (MAGTF) would have established, in some capacity, a command and control relationship with the cyber defense organizations of the JTF Commander, the theater Marine Forces Commander, and Marine Forces Cyber Commander. It is debatable which commander has the ultimate authority and responsibility to direct changes to the defensive posture of the MAGTF networks supporting the JTF. Each of the service components within the JTF has similar issues.

Along with a Geographic Combatant Commander, a newly designated JTF Commander has additional challenges he must understand at the beginning of the operation. All of the services employ their computer networks and support organizations just different enough to make coordination and sharing of a cyber common operating picture extremely difficult at best. A Joint Force Commander currently has the ability to visualize where his forces are arrayed in a Joint Operating Area. He lacks this visualization in the cyber domain. At best, he has a static display with stale information depicting which systems are operational and where intrusion incidents occurred. He lacks an accurate and dynamic cyber common operating picture, which

can overlay with his common operating picture for the other warfighting domains. Simply put, he does not know if unit X is at risk due to a vulnerability in cyberspace. He also lacks the ability to effectively command and control the networks within his Joint Force. If one were to follow the elder Helmuth von Moltke's concept of campaigning, the Commander already has failed before the operation begins because he has not established the proper conditions before commencing the campaign.[1]

One of the conditions the JTF Commander has failed to establish up front is that he is unable to ascertain the baseline security posture across the entire force. Unfortunately, he cannot establish what normal network activity looks like throughout the JTF. All of the computing devices and software applications in his command are of varying types, models and series with all of the incumbent security vulnerabilities.[2] Cyber defense planners within the JTF's operations division have significant challenges to overcome prior to developing a coherent plan in support of the JFC's campaign objectives.[3]

Five Disadvantages

Before discussing how the joint warfighting principles may be applied to the cyber domain, it is important to understand what a JTF Commander and his planners face as they begin designing a plan. In developing their portion of a campaign plan, cyber defense planners face no less than five inherent disadvantages. They include, but are not limited to, the advantage in cyberspace residing with the offense, the difficulty in sharing cyber security information between security agencies within the JTF, the presence of multiple adversaries in the domain, a reliance on the Internet for critical support functions, and a lack of understanding of the cyber domain's characteristics.

In the cyber domain, the advantage resides in the offense. An attacker can bide his time, shape the environment, and strike at the time and place of his choosing. In contrast, cyber defenders must be vigilant in a 360-degree defensive posture. A similar dynamic exists between insurgent and counterinsurgent. Counterinsurgency theorist David Galula argues that an insurgency is relatively cheap compared with the costs of counterinsurgency.[4] In an insurgency, a relative advantage resides with the insurgent in that the insurgent can hide within the general population and can wait for the best time to strike. Galula's description is applicable to the cyber domain. Comparatively speaking, an attacker's tool set is relatively cheaper than a defender's aggregate cyber defense requirements.

Similar to an insurgent's activity, a cyber attacker's activity can hide within legitimate network activity. In the cyber domain, an attacker can be selective in evaluating which attack methodology would be the most effective. The easiest way for an adversary to gain access to a DoD network is exploiting human nature. In a possible scenario, an adversary attempts to deliver malware via what is known as a phishing email. The adversary successfully targets and delivers malware to a key member of the JTF staff. Believing an attachment is legitimate, the staff member clicks on the malware beginning the process whereby the adversary gains access to the DOD network via the victim's computer and is able to navigate the network. This malware enables the adversary to access files remotely and send them outside of the DoD network. The adversary may also be able to access key files and modify them in a way where the modifications would not appear out of the ordinary, but nonetheless makes the friendly force take the adversary's desired actions. A worst-case scenario is when the adversary is able to escalate his network privileges to that of a network administrator and can create new accounts and implement network security modifications at will. This worst-case scenario is the functional equivalent to

having an enemy agent operating within the command with unfettered access to key personnel and documents.

A JTF Commander can assume similar events as the scenario described above are occurring within each of the JTF service components. It is difficult to establish a trend of whether the individual incidents at each of the service components are isolated events or a coordinated series of initial shaping actions of a larger attack in the cyber or other warfighting domains. This limitation is due largely to the previously mentioned lack of cyber common operating picture and information sharing shortfalls between cyber defense organizations. It is likely that the JTF cyber defense organizations have not previously worked together and have not established useful information sharing processes before the operation began.

Cyber defense planners also face a multitude of adversaries within the domain. While a JTF Commander will likely have a designated adversary for his operation, additional adversaries can strike the JTF as well. For example, there may be cyber activists, cyber patriots or other opportunists who may rally to the aid of our enemy via the cyber domain. The cyber domain expands a JTF commander's area of interest significantly.

A JTF Commander's area of influence is also larger than normal because the Department of Defense relies on Internet connectivity with commercial providers to support logistics requirements. The DoD must maintain open communications channels to keep the joint force supplied. Additionally, the United States' reliance on information technology provides potential adversaries an unprecedented level of access to the joint force service members.[5] An adversary can use the indirect approach to reduce a JTF's combat effectiveness.

For example, the DoD pays most of its service members via direct deposit disbursing funds directly into members' bank accounts. The direct deposit system provides adversaries

opportunities to influence a JTF's effectiveness. A review of recent newspaper reports of computer security breaches at major financial institutions gives one an appreciation of the potential impact an adversary could have on the military's morale and combat effectiveness via cyber attack.[6] One need only imagine the effect of having widespread pay outages to military members while they are deployed. Military members could be distracted by news from spouses that salary payments have not properly been distributed.[7] Media reports from home station can affect troop morale. History can provide examples of the effect media reports from the home front can have on front line troops.[8]

The fifth of the cyber defense planner's challenges is the JTF members' fundamental lack of understanding of the characteristics within the cyber domain. In the past, military units would display posters depicting the Soviet order of battle and plates of information on the prevailing Soviet weapons systems. There was an implicit understanding that everyone was responsible for learning the information displayed. The implication was everyone could develop collective technical and tactical proficiency by study and familiarization. This shared proficiency is not the case today in the cyber domain. While one may hear of cyber attacks in the news and have to complete annual training, the repetitive discussion and familiarization of the adversary's order of battle does not occur. It may be the joint force does not really understand what it is collectively up against on a daily basis. This gap in technical understanding and the other four disadvantages will make operational art in the cyber domain more difficult.

Understanding the environment

Just as in the other warfighting domains, an operational planner must understand the environment. Actions taken within the cyber domain can have disproportionate outcomes. The disproportionality is the result of adversary having a high-speed avenue of approach to JTF

information. Unlike the other domains, adversaries have weapons parity with the United States in cyberspace. An adversary need not spend significant resources to develop strategic weapons to inflict damage. He requires only a laptop and an Internet connection to begin his campaign.[9] If a JTF is unable to trust the information that is available within its networks, it is unable to maximize the JTF's combat power.

An operational planner will be challenged to make the linkage between strategic objectives and tactical actions within the cyber domain without a solid foundation of the technical capabilities and limitations of cyber operations. The gap is artificially induced by a general unwillingness to discuss detailed cyber capabilities openly. Similar to nascent nuclear weapons doctrine, an element of ambiguity is somewhat necessary. As long as the DoD continues to limit the dialogue to closed-door sessions, it cannot leverage the collective brainpower of the individual service members to develop well-reasoned solutions.[10]

A JTF Commander may be tasked to support the host nation defend its networks during an operation. This task would be similar to supporting a foreign internal defense mission. However, the Commander must understand that he has limited resources to achieve this objective. He cannot project combat power to defend a host nation network. The Commander can only facilitate the improvement of network defense activities by suggesting and coordinating industry best practices for the host nation.[11] Similar to intelligence sharing, information sharing for the cyber domain with partner nations is problematic.

The question of whether network intrusions constitute an attack, espionage or criminal activity needs to be codified to help establish what the Commander can do in response to the activity. In short, it is difficult to establish clear rules of engagement in the cyber domain. There is little agreement on what constitutes acceptable behavior in the domain. Part of the challenge

of what constitutes a provocative act is how policy makers and military leaders view attacks against networks.[12] Most cyber intrusion activity can be classified as intelligence collection efforts or electronic warfare. One is both a warfighting function and national security activity; the other is an act of war. The results of cyber activity would determine whether or not the activity was an act of war or simply an activity supporting war. For example, the production of food and clothing is not by definition warfare. However, the distribution of food and clothing to front line troops is a key warfighting function and to deny the enemy the same would constitute warfare. The question of whether distributed denials of service (DDOS) are an act of war or are they to be considered criminal activity has not been resolved. Like terrorist activity, actions can be viewed through both a criminal lens while other times the activity can be viewed through a warfighting lens. Both views have different decision chains that are not always mutually supporting. If leaders view the events as criminal activities, then rules of evidence and jurisprudence would normally apply. If decision makers view the activity as warfare, a JTF could take aggressive defensive countermeasures in response to the activity.

Similar to conflicting views of what constitutes acceptable behavior in the domain, there remains disagreement of the role of the domain in war. Clausewitz argued that war is a continuation of politics by other means and that without violence or the threat of violence, there is no war.[13] A student of war and warfare could have difficulty understanding the role of operations in cyberspace using Clausewitz's model. His theory remains relevant. Cyberspace has a role in war in that cyberspace is simply a means to achieve both political and military objectives. Similar to the physical domains, offensive and defensive operations have a role in war. In the cyber domain, defensive cyber operations can only be a combat support effort. Cyber defense activities can affect the outcome of an operation in a similar manner as

operational security and counterintelligence efforts. The means cyber planners and operators employ to achieve their objectives are part of the art and science in war. Use of the cyber domain is not much different than use of any of the other warfighting domains to achieve an objective. Each domain has its own characteristics, but ultimately the actions in each domain must support overall operational objectives.

A JTF Commander is nearly blind to any cyber activity outside of his own networks. His visibility to see beyond his network activity is limited because the outside networks are owned and administered by private organizations. He can try to clear the fog with surveillance tools. However, he is limited to what his friendly intelligence efforts are able to provide. It is difficult to know if a cyber actor is massing a botnet for a deliberate DDOS attack or if an adversary is developing a new phishing campaign targeting key leaders. While this type of activity occurs almost daily, it is difficult to establish what the normal noise level is and to compare it to something extraordinary. Without understanding what normal looks like, an operational planner will struggle to gain an advantage in cyberspace.

The JTF's role in protecting commercial network systems in a host nation is uncertain. It is well known the United States military relies on commercially provided network services and support activities. Since commercial vendors provide network leases, the data passes through private American and foreign company communications equipment.[14] While the DoD uses robust encryption methods to mask the data, an adversary need only cause physical destruction of a few key network intersections to degrade US operations. One could argue that protecting a critical network node is similar to protecting a major utilities facility within the Joint Operating Area. One could also argue that the host country should protect these key network nodes themselves. However, if the host nation does not have an adequate capability to defend the

nodes, the question of whether the JTF could perform a type of cyber foreign internal defense comes to the fore again.

At the operational level, a JTF Commander should understand how his networks interact with the larger DoD networks and how the DoD connects to the Internet to support a campaign. The DoD uses Internet Access Points (IAP) as gateways between government networks and the Internet. There are relatively few IAPs in the DoD, but the volume of information that travels across them is great. For the United States, these cyber choke points have the strategic equivalence of the straits of Gibraltar or Malacca. Should an IAP become unavailable, the DoD's logistics and supply chain could become severely degraded. Over time, the DoD would begin to lose combat effectiveness if it were not able to openly communicate with vendors and mission partners.

Throughout the DoD including the JTF level, sub-organizations establish logical network boundaries using a variety of methods. The purpose of this defense in depth strategy is to limit the risk between organizations. In other words, a risk to organization A does not necessarily impact organization B even though the two organization's respective networks are connected. While this approach is generally effective in containing security risks, it does come at a cost in reduced information sharing. To share information between organizations, network administrators must assign rules to allow varying levels of information access between organizations. The challenge grows as the administrators must establish access rule sets between multiple organizations and maintain constant vigilance to ensure the rule sets are updated.

A similar process occurs between the cyber security organizations. Many DoD organizations have personnel dedicated to monitoring security logs and intrusion attempts. Each security organization would have to establish security rules sets between themselves to

understand better what is happening in their adjacent organizations.[15] This process is akin to a rifle company commander understanding what his sister rifle companies are experiencing while they are all in a defensive posture.

However, there is such a thing as too much information in cyber defense. Some cyber defense planners believe that access to all of the security data available will help reduce the fog of network security incidents. The problem with this line of thinking is the shear volume of security events occurring at all levels between the outer boundary at the IAPs, the JTF and service component level can quickly overwhelm the JTF equipment and security staff. Another approach to consuming and analyzing network security alert data is a division of labor between hierarchal security organizations. Far from perfect, this alternative approach presents a flaw of each organization having a myopic perspective to security alerts and activities.

Warfighting Principles In the Cyber Domain

Unlike the other warfighting domains, cyberspace is man-made and has unique characteristics. An operational planner may find it useful to examine how the warfighting principles of mass, objective, offense, security, economy of force, maneuver, unity of command, surprise, speed (MOOSEMUS) apply as a framework in conceptualizing how he and a cyber defense planner would design a cyber defense plan for a Joint Task Force. Careful consideration of the principles reveals that they do apply to the cyber domain. This section will demonstrate how planners may apply the principles.

Arguably, mass is the most difficult principle to apply to cyber defense. An organization cannot mass its forces to meet a new threat. The cyber defense infrastructure and personnel expertise are in place or they are not. One possible way to mass forces would be to increase the collective understanding of all members of the Department of Defense beyond the minimal

computer based awareness training currently in place.[16] The collective cyber training requirements within the DoD are inadequate and directly contribute to the lack of understanding personnel have of the domain's characteristics. As a comparison, the public would think the services as negligent if the amount of weapons handling training were diminished to the levels currently required for annual information assurance training. If every member of the department understood the safe handling of the network components, the DoD could greatly diminish the security risks to the network.[17] These better-trained military members would report for duty with a Joint Task Force better prepared to take an active role in defending the cyber domain or at a minimum not aiding the adversaries unknowingly.

The next principle to review is the principle of objective. A JTF must have clear objectives for operating in the cyber domain. Clearer objectives would assist an operational planner in developing a coherent a cyber defense campaign. At present, the DoD uses many directives in an attempt to articulate what it desires for the cyber domain. The Marine Corps' Cyberspace Concept of 2009 recognizes a fundamental gap and lack of integration between strategic and operational objectives.[18] The 2011 DoD Strategy for Operating in Cyberspace, lists four broad security objectives. While a step in the right direction, the four objectives still do not translate into coherent operational objectives and tactical tasks.[19]

In the absence of clear objectives, a Commander may consider defending other key network nodes within his Joint Operating Area along with JTF networks. Brett Williams, the former Pacific Command J6, is correct in his *Joint Forces Quarterly* article when he argues a Joint Force Commander must consider elements of the cyber domain when evaluating key terrain, centers of gravity and critical vulnerabilities.[20] However, he goes astray in asserting that a JTF Commander cannot defend all components of a JTF network; the Commander must. In the

cyber domain, an adversary needs to be successful once to be effective. The DoD's defense in depth strategy is an effort to make intrusions and exploitation more difficult for the adversaries. The risks associated with limited defenses of cyber networks have the potential to be more significant than the loss of an aircraft or vehicle. A better argument can be made that a JTF Commander apply more resources in defending key cyber terrain and develop contingency plans should key network node be made unavailable. A JTF Commander should have contingency plans in place to work through the loss. He would do the same for any critical resource or key terrain in the other warfighting domains.

While attempting to develop clear operational objectives, it is generally believed that a Commander who defends everywhere defends nowhere. This belief should not be applied to the cyber domain. A Commander must assume some measure of risk. However, the risks associated with a poor defense strategy in the cyber domain have outsized impacts compared to the land, maritime and aviation domains. For example, a lightly defended area in the land domain may allow the commander to make a calculated risk that an adversary cannot exploit the area before the friendly force can respond. The speeds at which cyber gaps can be exploited are much faster than what operators are normally accustomed to.

All members of a Joint Task Force, in addition to cyber defenders, must have an offensive spirit in the pursuit of effective cyber defense. This is not to be confused with taking a first strike at an adversary. First strikes as part of an active defense campaign could prove useful, but the subject is beyond the scope and classification of this paper. Cyber defenders can take an active role further by reviewing internal network activities to determine what activity is legitimate and what activity is not. Cyber defenders need to view themselves as more than network administrators. They need to embrace their operational relevance to the warfighting

effort as operational contributors and not a supporting function. Likewise, all personnel within a JTF have an active role to play in defending the cyber domain. A JTF should have clear guidelines for how individuals can take an active role. For example, the JTF can establish easy reporting procedures for suspected adversary activity and daily reminders of adversary trends.

The next principle to consider is the principle of surprise. As previously stated, the attacker has the upper hand in the cyber domain. The attacker can use surprise to his advantage by carefully planning and shaping the conditions to launch an attack largely unnoticed by the defender. The defender must remain ever vigilant to all adversary activity. The attacker also has an advantage in that he could use of form of surprise by exploiting what is known as a zero-day vulnerability or social engineering to launch an attack.[21] The defender may not be aware of the vulnerability until it is too late to implement a remedy. To minimize the adversary's use of surprise, operational planners must realize that software patches and secure configuration settings are an operational issue that are as important as fuel or ammunition levels and must be viewed as a means to thwart an adversary attack vector.

Much of the dialogue about the cyber domain tends to focus on offensive cyber capabilities. As a result, cyber defense is relegated as an economy of force effort. However, a poor cyber defense effort can be a critical vulnerability for a Joint Task Force and should not be an economy of force effort. Cyber defense is arguably the most important component a Commander needs to understand to support his overall campaign and should not make it a lesser activity by focusing solely on offensive cyber activities. Increasing his understanding is important because of how much a JTF relies on networks to operate in all of the warfighting domains. The cyber defense effort cannot continue to be downgraded as something the communications technicians handle.

A review of the Marine Corps Concept for Operating in Cyberspace reveals a gap between computer network defense and defend functions under the auspices of Network Operations.[22] This gap is more than temporal on a diagram. The gap represents a significant misunderstanding within the operations community that there is a difference between computer network defense and communication network operations. Until this gap is closed, there will remain limits to having a holistic understanding of what an adversary is trying to do to a Joint Task Force during a network attack. If for example a critical fiber optic cable line is cut, cyber defenders should attempt to correlate whether the cut is due to routine environmental conditions or part of a coordinated cyber shaping actions. The people who conduct the defend tasks in communications network operations are normally the same individuals who do computer network defense. Cyber defense is an operational issue that cannot continue to be relegated as an economy of force effort.

During the 2008 conflict between Georgia and Russia, the Georgians used a form of maneuver to defend their cyber presence. Unlike the Estonians who in 2007 decided to defend in place during a cyber attack they experienced, the Georgians maneuvered some of their cyber presence to the United States via private corporations.[23] This option raises a couple of issues future Joint Task Force Commanders may have to face should another country take similar action. First, the Georgians expanded the operating environment to the continental United States, which had not been previously involved in the cyber attack. The Georgian action complicated the operating environment further by inserting the United States between two belligerents before US policy makers can determine if the United States had a vested interest in intervening. It would be difficult to imagine the United States or any country not taking an interest in such actions after they occur. This maneuver is akin to the Germans, upon initiating

World War I, marching through Belgium and the Allies not aiding Belgium in the process of defending France. The result of a limited response could be similar to the United States' experience in fighting the Vietnam War by limiting activity in Laos during the early stages of the war.

A second aspect of maneuver a JTF Commander may have to consider is how quickly he can change the network in response to adversary action. Much of the network support a JTF enjoys is often provided by contract support. A network configuration or application of a security patch can have significant impact to mission capabilities, take time and increase financial costs. For example, a vulnerability remedy can inadvertently render an application feature useless. A cyber defender must be able to explain quickly and clearly the technical impact of a network change to help determine the operational impact of the change.

A third issue created by maneuvering in cyberspace that may vex a JTF Commander is the issue of aid and comfort provided by a third party. Like many support activities, it is difficult to parse accurately and consistently which dual use materials and functions offer strictly humanitarian support and directly support war aims. In the example of the Georgians moving their cyber presence to private corporations within the United States, the purpose of the cyber presence would determine if the private companies provide material war aid or humanitarian aid. There is a difference if a Twitter account or blog site hosted in the United States is directing the humanitarian relief effort or being used as a method of national command and control functions. The difference between the two puts a third party's host government in an awkward position.

A Joint Task Force Commander may have trouble establishing a unity of command within the cyber domain, which is arguably the most important warfighting function. Simply, the answer to the question of who is in charge is not always apparent. There are multiple

organizations with a stake in the cyber domain. US Strategic Command has responsibility for the cyberspace mission area that is subsequently executed by US Cyber Command. US Cyber Command was established as a sub-unified command to focus on the cyber domain. Each of the military services has a cyber component command in support of US Cyber Command. The Defense Information Systems Agency is responsible for defending a significant portion of the department's computer networks since they provide the bulk of the military's access to the Internet. Geographic combatant commanders may all believe they are responsible for the cyber domain within their respective areas of responsibility. A Joint Task Force Commander also believes he is responsible for the cyber domain within his Joint Operating Area. The problem is they are all correct. The solution to answering the question of who is in charge may reside in establishing a standing Functional Cyber Component Command within each of the geographic combatant commands.

Related to unity of command, the speed of events within the cyber domain is faster than most people can comprehend. Therefore, traditional command and control relationship models of transitioning changes of operational control of "cyber forces" when they are needed do not apply. A Combatant Commander would be well served in establishing a standing Functional Cyber Component Command. A standing Functional Cyber Component Command would allow the combatant command to better support any Joint Task Force Commander during contingency operations by resolving command and control relationships before a crisis occurs. Part of the command and control confusion resides with the issue of each military service component having integrated cyber support organizations within the service components. This type of problem has been addressed before within the DoD. There is a similar challenge in how the joint force employs aviation assets. It took the DoD many years to develop current doctrine for

supporting the Joint Force Aviation Component Commander (JFACC). Others, such as Williams suggest a Special Operating Forces model would be a better solution for the lack of a sound command and control structure in the cyber domain.[24] A final command and control construct would likely have elements of how the JFACC and the Theater Special Operation Commander command and control forces to support a Geographic Combatant Commander today.

In a time of constrained fiscal resources, it is unlikely that the military services would be willing to defer command and control responsibilities for the cyber domain to another military service. Each service component commander believes that he is responsible for his portion of the cyber domain and needs the flexibility to operate within it to support his objectives. Perhaps an update to the Goldwaters-Nichols Act is needed to facilitate changes within the military departments to ensure effective command and control structures are developed for the cyber domain.

The final principle to consider is security. Establishing the proper security levels within a Joint Task Force network can be problematic. There exists a tension between network security administrators and operations personnel in attempting to balance the operational needs of the organization with minimal risk to security. A JTF Commander has to balance the requirement for keeping security levels adequate to allow network functionality. The security-balancing act directly affects the simplicity of security measures for individuals to employ. Security measures must be simple enough to be employed during daily use of the network and countermeasures easily implemented if security is breached. A Commander will have to establish security protocols that do not make using the network too difficult for the average user. If the security protocols are too cumbersome, people within the organization will likely try to bypass security measures creating a bigger problem than the one the JFC is trying to solve.

The Campaign Plan

Considering all of the inherent challenges and characteristics of the cyber domain, planners can apply the tenants of operational art to develop a cyber defense plan as part of an integrated theater campaign plan. Joint force planners need to understand where the force's cyber defense posture is starting from and what the end-state is to be. Planners must have a strong foundation of the characteristics of the cyber domain.

It is debatable if action within the cyber domain can be decisive or the main effort of the entire campaign. Williams rightly argues that cyber defense at the operational level can be the main cyber effort.[25] Actions in the cyber domain can be the main effort during early phases of a campaign. Shaping actions in the cyber domain can prepare a JTF for future actions in the domain. If the Commander designates cyber defensive efforts as the main effort in an early phase of an operation, he can set the conditions to protect his networks so their future use in subsequent phases can properly support his campaign.

A JTF cannot operate in a single domain to achieve its objectives. As noted author Colin S. Gray points out, the state does not wage war in a single domain.[26] A domain must be integrated with all of the warfighting domains. Dominance in a single domain only contributes to the overall outcome of a campaign. Such is the case for the cyber domain. Planners must design a cyber defense plan that supports the objectives in the other warfighting domains.

Operational planners must have an appreciation a Joint Task Force's network security posture to develop a campaign plan. It would be ideal if each service component had an accurate assessment of how vulnerable they were to network attack immediately upon the release of new network threat. The nature of networks and software is such that it is extremely difficult to understand an organization's risk because of the prevalence of hardware and software coding

errors. For example, each organization has to know precisely the type, model, and series of all operating systems, hardware and software applications they have running within their networks. Any number of the above listed areas can have both identified and unidentified security risks because of faulty programming. When vulnerabilities are uncovered, it is common for remedies to not be available in a timely fashion. The absence of understanding how vulnerable an organization is makes developing a coherent campaign plan complicated. The Defense Information Systems Agency (DISA) is working to make secure configuration management and continuous monitoring easier for the cyber defender.[27] The JTF must be able to integrate the available information to clear the operational picture for the Commander.

While developing a cyber defense campaign plan, planners must understand the capabilities of interagency partners in addition to all service components. Current law prohibits the Department of Defense from defending commercial entities in the cyber domain. A significant concern is that the defender normally has access to the data systems it is responsible for defending. The defender will normally have to review transaction logs to determine which connections may be the source of adversary activity. Further complicating matters, the Department of Defense is not mandated to provide cyber defense to other sectors of the US government. The DoD is working with the Department of Homeland Security (DHS) to develop best practices for defending other elements of the US government networks.[28] The outcomes of these best practices should benefit the JTF Commander in the future. Ideally, the two departments can develop an information-sharing process that would give the United States better situational awareness of what adversaries are attempting to do to government networks. The work between the DoD and DHS will help clarify what each organization is responsible for. If other elements of the US government are responsible for defending non-DOD networks,

information sharing amongst the interagency cyber defense organization can help lift the fog of what is occurring within the cyber domain for the JTF Commander. Coordination similar to the interagency information sharing process is important so a JTF can design and execute a cyber defense plan.

The department's reliance on social media further complicates the cyber defender's job. Use of social media to communicate the Department of Defense's public message increases its risk. While key billet holders within a Joint Task Force have a need to access social media sites, most service members within a JTF do not need continuous access to social media to perform their duties. Access to social media contributes to the defense workload. The more traffic traversing the Internet Access Points, the more data that has to be monitored and evaluated for malware and adversary activity. A Commander may consider limiting the JTF's general access to social media, which is counter to prevailing directives.[29] If the Commander reduces non-mission critical network traffic, the cyber defenders can improve the quality of the defense effort by dedicating resources that would have been used to inspect frivolous network traffic to improve the quality of defense of mission essential network traffic. Critics may counter that access to social media sites is needed to help tell the military story and keep morale high. This argument is a compelling reason to allow all JTF members to have access to social media, but the counterpoint is that access to social media sites need not be available at undue government risk. Planners should design a separate morale network solely for the purposes of accessing non-mission critical sites for the general JTF population. This network should be directly connected to the Internet predominately for recreational purposes.

Many operational planners struggle to embrace the concept of data integrity.[30] Many planners believe that network intrusions predominately consist of exfiltration data. While that

belief may be mostly true, it is not the most significant type of intrusion. The author's experience during exercises was most operational planners believed adversary knowledge of friendly information was irrelevant because the adversary could not affect the outcome of the plan.

The value of data is rooted in its accuracy. When considering data integrity, a touch of paranoia is healthy. As there are levels of sophistication in burglary, there is equal sophistication in adversary capability. How does one know if their house was broken into while they were away and something valuable was taken or altered if the burglar left little evidence? Likewise, how is one to know if an adversary is copying, reading and modifying the files on JTF computers or planting disinformation? These questions must be resolved prior to an operation.

Should a security breach be discovered, operational planners must understand the characteristics of the breach and cyber defenders must be able to clearly articulate how the breach could affect an operation. Thinking the enemy knows a Joint Task Force's plan, but cannot do anything about it is not always the appropriate assessment. Sometimes the severity of the security breach can be comparable to a situation where the enemy modified the characteristics of the JTF's artillery shell/fuse combinations or contaminated fuel sources. Operational planners must ensure the cyber defense force has the necessary resources to protect data integrity and the underpinning concepts to support the operational plan. There are security-monitoring tools to lighten the burden on cyber defense organizations. Cyber defender must constantly tune and adjust these tools to make them effective just as any other operator would refine and tune his weapons systems.

Similar to the other domains, cyber defense planners are well served by thinking of the enemy first. The cyber domain's characteristics enable multiple adversaries to attack a Joint Task Force while it is attempting to conduct operations in the physical domains. The most significant

challenge for a defender is determining attribution for a breach in his network. An attacker can mask his activity using a variety of methods. Unlike a missile strike where a defender can study a missile's trajectory to understand who just attacked, a cyber defender cannot always do the same. Often, "cyber patriots" or sympathizers rally to an adversary's cause. Opportunists may try to learn how a Joint Task Force would operate in the cyber domain in preparation of future conflicts. In some respects, a Joint Task Force is surrounded in the cyber domain. Planners must prioritize which cyber adversaries they will focus the defensive effort on. Admittedly, this obstacle is extremely difficult to overcome given the resources a JTF normally has available. A Commander may have to accept early in an operation that he may never know who is accessing his networks.

Establishing a standing Functional Cyber Component Command in each of the geographic combatant commands will enable operational planners to develop strategies to prepare for future operations. A standing command, properly resourced, would have the ability to develop and exercise standing operating procedures to counter adversary activity before a crisis. A standing Functional Cyber Component Command can reduce some of the disadvantages a JTF Commander faces by having clear command and control relationships established and presenting a clearer cyber defense picture. The proposed command would also provide a JTF Commander an estimate of how the JTF could operate in a degraded cyber environment.

A Joint Task Force Commander, as the supported commander, would need to reconcile how severe of a deliberate cyber attack his JTF can withstand and remain combat effective based on the cyber component command's framework. This effort is no trivial task. Most service members take command and control systems for granted. Commands make little effort to learn

how long a joint force can be effective in a severely degraded cyber environment. A Commander must establish redlines for the loss of certain command and control systems just as he would with the loss of a carrier or an aircraft wing and develop contingency plans.

Once an adversary employs a tool to access a JTF network, the tool is of little value as soon as the vulnerability that the adversary exploited is discovered. In essence, the attack has reached its culminating point. Williams counters that an attack does not reach a culminating point in the cyber domain.[31] However, the effects an attacker is trying to achieve will quickly diminish once the exploit is unleashed, the effort discovered and the defender takes remedial action. In other words, the defender can quickly develop a plan to counter the effort once the trap has been sprung. After a zero-day exploit has a patch, it no longer presents a viable threat. In a way, the adversary reached a culminating point in his cyber attack with a specific tool. The JTF will need to act quickly to help facilitate the adversary's culminating point. Similar to being caught in an ambush and executing a counter-ambush battle drill, a JTF must have a clear battle drill to develop solutions to network intrusions.

Conclusions: A Joint Task Force Commander can use similar planning tools and methods to defend the cyber domain as he would in any of the warfighting domains allowing for some of the unique characteristics of the domain. However, there needs to be a greater understanding within the operations community of the domain's characteristics to improve the combat effectiveness of a JTF. The cyber defense community also bears responsibility to understand its role as warfighting operators and not simply support technicians. While cyber defenders' contributions to the campaign may not garner headlines, the work these quiet professionals perform can have a profound impact to a JTF's success. Both the operational and

cyber defense communities have made significant strides to understand each other to better support their commands.

The Department of Defense will need change how it to organizes, trains and equips the military departments to support a theater campaign by providing the Commander the tools he needs to prevent the cyber domain from becoming a critical vulnerability. If the DoD cannot develop an adequate command and control model to support a JTF Commander earlier in an operation, it is likely that new legislation such as an update to Goldwater-Nichols is needed. The DoD must also improve how it trains the joint force so that its members can be prepared to play an active role in defending a critical resource.

Notes

[1] Bradley J. Meyer "The Elder Moltke's Campaign Plan for the Franco-Prussian War," *The Operational Art: Development in the Theories of War*, edited by B.J.C. McKercher, and Michael A. Hennessy, 29-49 (Westport, CT: Praeger Press, 1996) 29.
[2] Commercial vendors are under pressure to deliver products to market before they are fully tested and evaluated. Software coding errors may not be obvious until much later after release to market. These factors make computers and software security a constant struggle to reconcile.
[3] In many commands, the cyber defense planners are part of the J6 directorate. This trend is changing as more commands recognize the value of cyber defense planning to the overall success of the campaign.
[4] David Galula, *Counterinsurgency Warfare: Theory and Practice*, (New York: Praeger, 1964) 6.
[5] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace.* (Washington, DC, July 2011) 1.
[6] Multiple news media outlets are reporting that major financial institutes are reporting that cyber hackers have breached their computer networks. http://www.washingtonpost.com/world/national-security/banks-seek-nsa-help-amid-attacks-on-their-computer-systems/2013/01/10/4aebc1e2-5b31-11e2-beee-6e38f5215402_story.html
[7] While this scenario may appear far-fetched to some, a guest speaker at Marine Corps University presented a similar scenario during a lecture after this monograph was drafted.
[8] James M. McPherson, *This Mighty Scourge: Perspectives on the Civil War*. (Oxford: Oxford Press, 2007) 158.
[9] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace.* (Washington, DC, July 2011) 3.
[10] Headquarters, Marine Corps. *USMC Cyberspace Concept*. (Washington DC, 2009) 7.
[11] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace.* (Washington, DC, July 2011) 9.
[12] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Forces Quarterly*, issue 63, (4th quarter 2011): 70-73.
[13] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984) 77.
[14] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace*. (Washington, DC, July 2011) 9.
[15] Headquarters, Marine Corps. *USMC Cyberspace Concept*. (Washington DC, 2009) 8.
[16] Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly*, issue 61, (2nd Quarter 2011): 10-17.
[17] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace*. (Washington, DC, July 2011) 6.
[18] Headquarters, United States Marine Corps. *USMC Cyberspace Concept*. (Washington DC, 2009) 7.
[19] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace*. (Washington, DC, July 2011) 6.
[20] Williams.
[21] A zero-day vulnerability is a new flaw in a portion of a computer network that exists due to a coding error or bug.
[22] Headquarters, United States Marine Corps. *USMC Cyberspace Concept*. (Washington DC, 2009) 11.
[23] Joshua E. Kastenberg and Stephen W. Korns, "*Georgia's Cyber Left Hook.*" Parameters, (Winter 2008-2009): 60-76.
[24] Williams.
[25] Ibid.
[26] Colin S. Gray, *Another Bloody Century: Future Warfare*, (London, UK: Phoenix, 2005) 169.
[27] http://disa.mil/Services/Information-Assurance/SCM
[28] Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace*. (Washington, DC, July 2011) 8.
[29] The Department of Defense recently relaxed standards for access social media sites using government computers.
[30] Shon Harris et. al., *All in One: CISSP Exam Guide*, 5th ed. (New York: McGraw-Hill, 2010) 52. As part of the information security field, data integrity is one of three fundamental principles of security. Data integrity is upheld when the accuracy and reliability of the information and systems are provided and any unauthorized modifications are prevented.
[31] Williams.

Bibliography

Allen, Ralph. "Piercing the Veil of Operational Art." *Parameters* (Summer 1995): 111-119.

Andrues, Wesley R. "What U.S. Cyber Command Must Do." *Joint Forces Quarterly*, issue 59, (4th quarter 2010): 115-120.

Arquilla, John and David. Ronfeld. *In Athena's Camp: Preparing for Conflict in the Information Age*. California: RAND, 1997.

Betz, David J. and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*, New York, NY: Routledge, 2011.

Brown, Gary D. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Forces Quarterly*, issue 63, (4th quarter 2011): 70-73.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

Carr, Jeffrey. *Inside Cyber Warfare*, 2nd ed. Sebastopol, CA: O'Reilly Media, 2012.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and what to do about it*. New York: Ecco, 2010.

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Translated by Michael Howard and Peter Paret. Princton, NJ: Princeton University Press, 1984.

Defense Information Systems Agency Campaign plan
www.dtic.mil/dtic/tr/fulltext/u2/a546040.pdf - 27k - 2011-10-11

Defense Information Systems Agency Strategic Plan
http://www.disa.mil/About/~/media/Files/DISA/About/Strategic-Plan.pdf

Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace*. Washington, DC, July 2011.

Galula, David. *Counterinsurgency Warfare: Theory and Practice.* New York: Praeger, 1964.

Gray, Colin S. *Another Bloody Century: Future Warfare*, London, UK: Phoenix, 2005.

Harris, Shon, Jerry Cochran, Michael J. Lester, and Bobby E. Rogers. All in One : CISSP Exam Guide. 5th ed. (New York : McGraw-Hill, 2010.

Headquarters, United States Marine Corps. *USMC Cyberspace Concept*. Washington DC, 2009.

Hersh, Seymour M. "The Online Threat: Should we be worried about a cyber war?" *The New Yorker* (November 1, 2010): 44-55.

Hollis, David M. "USCYBERCOM: The Need For a Combatant Command versus a Subunified Command." *Joint Forces Quarterly,* issue 58, (3rd Quarter 2010): 48-53.

Korns, Stephen W. and Joshua E. Kastenberg. "*Georgia's Cyber Left Hook.*" Parameters, (Winter 2008-2009): 60-76.

Lambeth, Benjamin S. "Airpower, Spacepower, and Cyberpower." Joint Forces Quarterly, issue 60, (1st quarter 2011): 46-53.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no.5 (October 1, 2010): 97-108.

McPherson, James M. "*This Mighty Scourge: Perspectives on the Civil War*." Oxford: Oxford Press, 2007.

Meyer, Bradley J. "The Elder Moltke's Campaign Plan for the Franco-Prussian War," *The Operational Art: Development in the Theories of War*, edited by B.J.C. McKercher, and Michael A. Hennessy, 29-49, Westport, CT: Praeger Press, 1996.

Miller, Robert A., Daniel T. Kuehl, and Irving Lachow. "Cyber War: Issues with Attack and Defense." *Joint Forces Quarterly* (2nd Quarter 2011): 18-23.

Newell, Clayton R. and Krause, Michael D. *On Operational Art.* Washington: Center for Military History, 1994.

Olson, John Andrea and Van Crevald, Martin. *The Evolution of Operational Art: From Napoleon to the Present*. Oxford: Oxford Press, 2011.

Rantapelkonen, Jari. "Virtuous Virtual War." *Cyberwar, Netwar and the Revolution in Military Affairs*, edited by Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright, 51-71. New York, NY: Palgrave Macmillan, 2006.

Stavridis, James G. and Elton C. Parker III. "Sailing the Cyber Sea." *Joint Forces Quarterly*, issue 65 (2nd quarter 2012): 61-67.

Thornton, Rod. *Asymmetric Warfare*, Malden, MA: Polity Press, 2007.

Thomas, Timothy L. "Google Confronts China's 'Three Warfares'." *Parameters,* (Summer 2010): 101-113.

Thomas, Timothy L. "The Chinese Military's Strategic Mindset." *Military Review*, (November-December 2007): 47-55.

Wass de Czege, Huba. "War by Internet: The Logic of Strategic Deterrence, Defense, and Attack." *Military Review* (July-August 2010): 85-96.

White House, *Cyberspace Policy Review*, The White House, Washington, DC. 2009.

White House, *The National Strategy to Secure Cyberspace*. The White House, Washington DC, 2003.

White House, *International Strategy for Cyberspace*, The White House, Washington, DC, May 2011.

Wu, Chris "An Overview of the Research and Development of Information Warfare in China," *Cyberwar, Netwar and the Revolution in Military Affairs*, edited by Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright, 173-198. New York, NY: Palgrave Macmillan, 2006.